連続群論輪読 第1回

村松研 B4　泉 祐太

群とは

- 集合 G であって次の条件を満たすもの
  - $c = ab\,(a, b, c \in G)$ という演算が定義され、その演算が『群の公理』を満たす

- $c = ab$ という演算はしばしば『乗法』と呼ばれる
- 一般には $ab \neq ba$

群の公理

- 次の3条件を『群の公理』という

1. 結合律
   $\forall a, \forall b, \forall c \in G, a(bc) = (ab)c$
2. 左単位元の存在
   $\exists e, \forall a \in G, ea = a$
3. 左逆元の存在
   $\forall a, \exists a^{-1} \in G, a^{-1}a = e$

無限群、有限群

- 群 G の元が無限個であるような群を『無限群』という
- 群 G の元が有限個であるような群を『有限群』という
  - G が有限群であるとき、その群の元の個数を『群の位数』という

可換群

- 群 G の演算が群の公理以外に以下の条件も満たしているときに、その群 G を可換群(アーベル群)という

4. 可換性

$$\forall a, \forall b \in G, ab = ba$$

- 可換群では、しばしば群の演算を $c = a + b$ と表記し、加法という
- 加法においては、単位元を『零』といい、0 と表記する
- 加法においては、逆元を『負元』といい、$-a$ のように表記する

群の諸性質(1)

- $(ab)c$ または $a(bc)$ と表記される、群Gの元はカッコを外してabcと表記できる
- 積の個数によらず適用できる

群の諸性質(2)

- 群の左単位元は右単位元でもある
- 群の左逆元は右逆元でもある
- $(a^{-1})^{-1} = a$

証明は次のスライド以降で行う

群の諸性質(2)
-左逆元が右逆元でもあることの証明-

$a \in G$とする。

$a^{-1}a = e$ (公理2)

$a^{-1}aa^{-1} = a^{-1}$

$(a^{-1})^{-1}a^{-1}aa^{-1} = (a^{-1})^{-1}a^{-1}$

$eaa^{-1} = e$ (公理3による)

$aa^{-1} = e$ (公理2による)

以上より、左逆元は右逆元でもあることが示された。

また、a^{-1}の逆元は公理3の形をみて、a であることが言える。

つまり、$(a^{-1})^{-1} = a$ が示された。(証明終)

群の諸性質(2)

-左単位元が右単位元でもあることの証明-

$$
\begin{aligned}
ae &= aa^{-1}a && \text{(公理3による)} \\
&= ea && \text{(公理3による)} \\
&= a && \text{(公理2による)}
\end{aligned}
$$

以上より、左単位元が右単位元でもあることが示された。(証明終)

群の諸性質(3)

- 方程式 $ax = b, ya = b$ は各々唯一の解を持つ。
- 単位元と、群の各元の逆元はそれぞれただ一つ定まる。

群の諸性質(3)
-方程式の解の唯一性の証明-

$a, b, x, y \in G$とし、x, yの2つを未知数とする。

まず、方程式$ax = b$(1とする)$, ya = b$(2とする) がそれぞれ解を持つことを示す。

$x = a^{-1}b\ , y = ba^{-1}$を方程式に代入すると、
(1の左辺) $= aa^{-1}b = eb = b =$ (1の右辺)
(2の左辺) $= ba^{-1}a = be = b =$ (2の右辺)

となるので、各々の方程式は解を少なくとも一つ持つことが示せた。

また、方程式を以下の様に変形し、左辺に未知数のみを残すことを考える。

$$\begin{aligned} ax &= b \\ a^{-1}ax &= a^{-1}b \\ ex &= a^{-1}b \\ x &= a^{-1}b \end{aligned}$$

となるので、この方程式に解は$a^{-1}b$の1つのみであることが示せた。

方程式2についてもほぼ同様に示せる。(証明終)

群の諸性質(3)
-単位元、逆元の一意性の証明-

$a, x \in G$をとる。

単位元 e は、方程式 $ax = a$ の解である。

また、a の逆元 a^{-1} は、方程式 $ax = e$ の解である。

方程式 $ax = b$ の解の唯一性より、上に挙げた方程式の解は高々一つしかない。

以上より、単位元と、各元の逆元はただ一つに定まることが示せた。(証明終)

べき乗の定義

- 群 G の元 a のべき乗を次のように再帰的に定義する。

$a \in G, m \in \mathbb{N}$とおく。
このとき、
$a^1 = a, a^{m+1} = a^m a$

- また、0乗と負数乗を以下の様に定義する。

$a^0 = e, a^{-m} = (a^{-1})^m$

群の諸性質(4)

- 前のスライドの定義のもとで、以下の(3),(4)式が成立する。

  a $\in G$　$p, q \in \mathbb{Z}$とおく。

  $a^p a^q = a^{p+q}$ (3)

  $(a^p)^q = a^{pq}$　(4)

群の諸性質(4)
-指数法則の証明-

指数 k に対する数学的帰納法で行う。

$a \in G;\ x \in \mathbb{Z}; k \in \mathbb{N}$ とおく。

1.$k = 1$ のとき

<1>$x > 0$ の場合

$$a^x a^1 = a^x a$$
$$= a^{x+1}$$ となり、成立

<2>$x = 0$ の場合

$$a^x a^1 = ea$$
$$= a$$
$$= a^{0+1}$$ となり、成立

<3>$x < 0$ の場合

$-x > 0$に注意すると、

$$\begin{aligned} a^x a^1 &= (a^{-1})^{-x} a \\ &= (a^{-1})^{-x-1} a^{-1} a \\ &= (a^{-1})^{-x-1} e \\ &= (a^{-1})^{-x-1} \\ &= a^{x+1} \end{aligned}$$ となり、成立

以上より、$k = 1$のときは(3)は成立。

群の諸性質(4)
-指数法則の証明(続き)-

2.$k=y$で(3)が成立すると仮定して、$k=y+1$のとき

$$
\begin{aligned}
a^x a^k &= a^x a^{y+1} \\
&= a^x a^y a \\
&= a^{x+y} a \quad &\text{(仮定による)} \\
&= a^{x+y+1} \quad &\text{(指数の定義による)}
\end{aligned}
$$

以上より、(3)は全てのkに対して成立。よって、(3)が証明された。

(証明終)

群の諸性質(4)
-指数法則の証明(続き)-

(4)式の証明を行う。

$a \in G; p, q \in \mathbb{Z}$とする。

1.$p \geq 0$のとき

$$(a^p)^q = \underbrace{a^p \cdots a^p}_{q個} \quad (指数の定義による)$$
$$= a^{p+\cdots+p} \quad ((3)式による)$$
$$= a^{pq}$$

2.$p < 0$のとき

$-p > 0$ に注意すると、

$$\begin{aligned}(a^p)^q &= ((a^{-1})^{-p})^q \\ &= \underbrace{(a^{-1})^{-p} \cdots (a^{-1})^{-p}}_{q個} \\ &= (a^{-1})^{-p-\cdots-p} \\ &= (a^{-1})^{-pq} \\ &= a^{pq}\end{aligned}$$

1,2より、(4)式は全ての整数に対し成立。
(証明終)